U.S. Department of Commerce, Patent and Trademark Office	Atty Docket No.	Application No.
	M-16094 US	10/521,741
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant(s)	
(Use several sheets if necessary)	Craig B. Gentry	
	Filing Date	Group
	January 18, 2005	2134

U.S. Patent Documents

*Examiner Initial		Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate
	AA	4,309,569	1/5/1982	Merkle			
	AB	5,432,852	07-1995	Leighton et al.			
	AC	5,590,197	12/31/1996	Chen et al.			
	AD	6,141,420	10-2000	Vanstone et al.			
	AE	6,618,483	09-2003	Vanstone et al.			
	AE	6,826,687	10-2000	Rohatgi			
	AC	6,886,296	05-2005	John et al.			
	AH	7,113,594	09-2006	Boneh et al.			
	AI	2002/0154782 A1	10/24/2002	Chow et al.			
	AI	2002-0025034	02-2002	Solinas			
	AK	2005-0246533 A1	11/03/2005	Gentry et al.			
	AL	2003/0081785 A1	5/1/2003	Boneh et al.			

Foreign Patent Documents

							Translation	
		Document	Date	Country	Class	Subclass	Yes	No
	AM	EP 1 051 036 A2	08-11-2000	EP				

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	AN	Dutta, Ratna et al. "Pairing-Based Cryptographic Protocols: A Survey" Cryptographic Research Group. 2004.
	AQ	GENTRY, Craig and SILVERBERG, Alice: "Hierarchical ID-Based Cryptography," 24 May 2002, pages 1-21, XP002396667.
	AP	N. Koblitz, *Elliptic Curve Cryptosystems*, MATHEMATICS OF COMPUTATION, Vol. 48, Number 177, January 1987, Pp. 203-209.
	AQ	Y. Dodis, M. Yung, *Exposure-Resilience for Free: The Hierarchical ID-Based Encryption Case.*
	AR	U. Feige, A. Fiat, A. Shamir, *Zero Knowledge Proofs of Identity*, 1987 ACM 0-89791-22 7/87/0006-0210, pp. 210-217.

Examiner	Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.

U.S. Department of Commerce, Patent and Trademark Office	Atty Docket No.	Application No.
	M-16094 US	10/521,741
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant(s)	
(Use several sheets if necessary)	Craig B. Gentry	
	Filing Date	Group
	January 18, 2005	2134

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	AS	S. S. Al-Riyami, K. G. Paterson, *Authenticated Three Party Key Agreement Protocols From Pairings*, 2002.
	AT	C. G. Gunther, A. B. Boveri, *An Identity-Based Key-Exchange Protocol*, pp. 29-37.
	AU	A. Fiat, A. Shamir, *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, 1998, pp. 186-194.
	AV	J.C. Cha and J.H. Cheon, *An Identity-Based Signature from Gap Diffie-Hellman Groups,* Cryptology ePrint archive, Report 2002/018, 2002. http://eprint.iacr.org/
	AW	N. P. Smart, *An Identity-Based Authenticated Key Agreement Protocol Based on the Weil Pairing,* CRYPTOLOGY EPRINT ARCHIVE, Report 2001/111,2001. http://eprint.iacr.org/
	AX	D. Boneh, M. Franklin, *Identity-Based Encryption from the Weil Pairing,* ADVANCES IN CRYPTOLOGY – CRYPTO2001, Springer LNCS 2139.
	AY	C. Cocks, *An Identity Based Encryption Scheme Based On Quadratic Equations.*
	AZ	J. Horwitz, B. Lynn, *Toward Hierarchical Identity-Based Encryption.*
	BA	M. Girault, *Self-Certified Public Keys*, 1998, pp 490-497.
	BB	L.C. Guillou, J. Quisquater, *A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory,* ADVANCES IN CRYPTOLOGY - EUROCRYPT'88, Lect. Notes in Computer Science, vol. 330, pp. 123-128, Springer Verlag (1988).
	BC	R. Blom, *An Optimal Class of Symmetric Key Generation Systems*, 1998, pp. 336-338.
	BD	C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, *Perfectly-Secure Key Distribution for Dynamic Conferences*, 1998, Springer-Verlag, pp. 471-486.
	BE	F. Hess, *Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes based on Pairings*, CRYPTOLOGY EPRINT ARCHIVE, Report 2002/012, 2002. http://eprint. iacr.org/.
	BF	K. Rubin, A. Silverberg, *Supersingular Abelian Varieties in Cryptology.*

Examiner	Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.

U.S. Department of Commerce, Patent and Trademark Office	Atty Docket No.	Application No.
	M-16094 US	10/521,741
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant(s)	
(Use several sheets if necessary)	Craig B. Gentry	
	Filing Date	Group
	January 18, 2005	2134

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	BG	W. Diffie, M. E. Hellman, *New Directions in Cryptography*, pp. 29-40.
	BH	A. Menezes, P. van Oorschot, S. Vanstone, *Chapter 12 Key Establishment Protocols*, HANDBOOK OF APPLIED CRYPTOGRAPHY, 1997, pp. 489-541.
	BJ	V.S. Miller, *Use of Elliptic Curves in Cryptography*, 1998, pp. 417-426.
	BJ	D. Boneh, B. Lynn, H. Shacham, *Short Signatures from the Weil Pairing*, Advances in Cryptology: Asiacrypt 2001 (LNCS 2248), pp. 514-532, 2001.
	BK	E. Fujisaki, T. Okamoto, *Secure Integration of Asymmetric and Symmetric Encryption Schemes*, Michael Wiener (Ed.): CRYTPTO'99, LNCS 1666, pp. 537-554, 1999.
	BL	A. Shamir, *Identity-Based Cryptosystems and Signature Schemes*, 1998, Springer-Verlag, pp. 46-53.
	BM	U. Maurer, Y. Yacobi, *A Remark on a Non-Interactive Public-Key Distribution System*, 1998.
	BN	G. Hanaoka, T. Nishioka, Y. Zheng, H. Imai, *A Hierarchical Non-interactive Key-Sharing Scheme with Low Memory Size and High Resistance Against Collusion Attacks*, THE COMPUTER JOURNAL, Vol. 45, No. 3, 2002.
	BO	G. Hanaoka, T. Nishioka, Y. Zheng, H. Imai, *An Efficient Hierarchical Identity-Based Key-Sharing Method Resistant Against Collusion-Attacks*, JSPS-REFT 96P00604, pp. 348-362.
	BP	A. Joux, A One Round Protocol for Tripartite Diffie-Hellman, W. Bosma (Ed.), ANTS-IV, LNCS 1838, pp. 385-393, 2000.
	BO	Sakai, Ryuichi et al., "Cryptosystems Based on Pairing", The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 26-28, 2000, SCIS2000 - C20.
	BR	Sakai, Ryuichi et al., "Cryptosystems Based on Pairing over Elliptic Curve", The 2001 Symposium on Cryptography and Information Security, Oiso, Japan, January 23-26, 2001, The Institute of Electronics, Information and Communication Engineers.
	BS	Sakai, Ryuichi et al., "Crypt schemes based on Weil Pairing," pp. 1-12.

Examiner	Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.

U.S. Department of Commerce, Patent and Trademark Office	Atty Docket No.	Application No.
	M-16094 US	10/521,741
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant(s)	
(Use several sheets if necessary)	Craig B. Gentry	
	Filing Date	Group
	January 18, 2005	2134

U.S. Patent Documents

*Examiner Initial		Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate
	BT	6,212,637	04-03-2001	Ohta et al.			
	BU	2005-0022102	01-27-2005	Gentry et al.			
	BV	2003-0179885	09-25-2003	Gentry et al.			
	BW						
	BX						
	BY						
	BZ						
	CA						
	CB						
	CC						
	CD						
	CF						

Foreign Patent Documents

							Translation	
		Document	Date	Country	Class	Subclass	Yes	No
	CF							

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

	CG	Okamato, "A Digital Multisignature Scheme Using Bijective Public Key Cryptosystems," ACM Transactions on Computer Systems, Vo. 6, No. 8, 11/1992, pages 432-441.
	CH	Boyd, "Multisignatures Based on Zero Knowledge Schemes", Electronic Letters, 10/1991, Fol. 27, No. 22, pages 1-3.
	CI	
	CJ	
	CK	

Examiner	Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.